Kleptographic Attacks on E-Voting Schemes

Marcin Gogolewski[1], Marek Klonowski[2], Przemek Kubiak[2]
Mirek Kutyłowski[2], Anna Lauks[2], Filip Zagórski[2]

[1]Faculty of Mathematics and Computer Science,
Adam Mickiewicz University, Poznań

[2]Institute of Mathematics and Computer Science,
Wrocław University of Technology, Wrocław, Poland

ETRICS 2006

Demands on voting systems

- *... introduce e-voting!*
- *... make elections easier for a voter*
- *...forget complicated systems!...*
- *... neither politicians nor most of the voters will understand you and accept the solution...*

Lessons from the past

Case example - remote controls for unlocking a car:

- initial solution - a 32-bit key (fixed for a car) transmitted in cleartext,
- *... forget complicated systems - cryptography or other academic stuff... . We design practical systems!*

Lessons from the past

Case example - remote controls for unlocking a car:

- initial solution - a 32-bit key (fixed for a car) transmitted in cleartext,
- *... forget complicated systems - cryptography or other academic stuff... . We design practical systems!*
- but stealing cars increased rapidly

A patch

- a 32-bit cryptography is weak -
  so let's upgrade it to 64-bit keys,

A patch

- a 32-bit cryptography is weak -
  so let's upgrade it to 64-bit keys,
- but stealing cars as easy as before
  - a stupid countermeasure

A patch

- a 32-bit cryptography is weak -
  so let's upgrade it to 64-bit keys,
- but stealing cars as easy as before
  - a stupid countermeasure
- now for unlocking a car a fairly complicated cryptographic protocol is used
- the car owners do not even care to understand it ...

Demands on e-voting schemes

correctness the votes are counted honestly
it does not matter who casts the votes, it matters who counts them

verifiability a voter can check that her vote was counted
why to vote since my vote will be removed anyway, auditable paper traces

Motivations

anonymity — voters preferences must remain hidden

your employer has friends in the committee, they may say him how you have voted

case Brasilia and paper traces

no vote selling — a voter cannot prove how he votes

case Birmingham, selling votes for 1 pound in local elections

System components

Typical parts of the system are:

- voting machines VMs, or a voter's private machine
- or/and registration machines RMs (in some schemes only),
- bulletin board(s) $\mathcal{BB}$,
- a network of mix servers.

Outline

Necessity of randomness in e-voting

- Basic property:
  without decryption keys of tallying authorities candidate's name cannot be derived from a ballot.
- deterministic encryption
  $\Rightarrow$ perform trial encryptions with the public key and compare with the ballot

Necessity of randomness in e-voting

- Basic property:
  without decryption keys of tallying authorities candidate's name cannot be derived from a ballot.
- deterministic encryption
  $\Rightarrow$ perform trial encryptions with the public key and compare with the ballot
- $\Rightarrow$ voters' choices must be masked by (pseudo)random values.

Necessity of randomness in e-voting

- Basic property:
  without decryption keys of tallying authorities candidate's name cannot be derived from a ballot.
- deterministic encryption
  $\Rightarrow$ perform trial encryptions with the public key and compare with the ballot
- $\Rightarrow$ voters' choices must be masked by (pseudo)random values.
- many such situations in cryptographic protocols

Dangers of randomness

It is known that freedom of parameters valuation makes room for a *subliminal channel*, through which may leak:

- voters' choices,
- signing keys of voting machines,
- ...

Kleptography I

- designed by Yung and Young ten years ago,
- perhaps the most important threat for security of high end systems
- implementation of “Big Brother” with only one TV receiver, while “Big Brother” remains perfectly hidden

Kleptography II

Kleptography makes the subliminal channel very selective:

- the channel is protected (encrypted) by a public key of a malicious Mallet,
- reading data from kleptographic channel with a secret key only,

Kleptography III

- non-invasive testing cannot detect klepto-code,
- reverse engineering of a device/software "compromises" only the public key, the private key is not there!
- how many tamper resistant cards you will check?
- the producer can always claim that this was not an original device

Kleptography IV

A perfect technology for corrupting elections.

It does not matter who casts the votes,
it does not matter who counts them,
the only thing that counts is who produces the voting equipment

Outline

The ballot in Neff's scheme

The ballot is a matrix of BMPs (*Ballot Mark Pairs*)

$$\begin{array}{|llll|}
\hline
\mathrm{BMP}_{1,1} & \mathrm{BMP}_{1,2} & \dots & \mathrm{BMP}_{1,\ell} \\
\mathrm{BMP}_{2,1} & \mathrm{BMP}_{2,2} & \dots & \mathrm{BMP}_{2,\ell} \\
\dots & \dots & \dots & \dots \\
\mathrm{BMP}_{i,1} & \mathrm{BMP}_{i,2} & \dots & \mathrm{BMP}_{i,\ell} \\
\dots & \dots & \dots & \dots \\
\mathrm{BMP}_{n,1} & \mathrm{BMP}_{n,2} & \dots & \mathrm{BMP}_{n,\ell} \\
\hline
\end{array}$$

where:
n is the number of candidates,
ℓ is a security parameter, $\ell \in \{10, 11, \dots, 15\}$.

The ballot in Neff's scheme

Each $\mathrm{BMP}_{j,k}$ is a pair $(b_{j,k,L}, b_{j,k,R})$ of ElGamal ciphertexts:

$$b_{j,k,\alpha} = (g^{\omega_{j,k,\alpha}} \;,\; m_{j,k,\alpha} \cdot y^{\omega_{j,k,\alpha}})$$

for $\alpha \in \{L, R\}$, where:

- (g, y) is a public key for mixes,
- $m_{j,k,\alpha} \in \{Y, N\}$, and Y, N are fixed elements: one of them is neutral element ("1"),
- $\omega_{j,k,\alpha}$ are <u>supposed</u> to be <u>random</u> values.

The ballot in Neff's scheme

Suppose that voter Alice has chosen a candidate C_i, then

- each $\mathrm{BMP}_{i,k}$ in the ith row

$$
\begin{array}{|cccc|}
\hline
\mathrm{BMP}_{1,1} & \mathrm{BMP}_{1,2} & \dots & \mathrm{BMP}_{1,\ell} \\
\mathrm{BMP}_{2,1} & \mathrm{BMP}_{2,2} & \dots & \mathrm{BMP}_{2,\ell} \\
\dots & \dots & \dots & \dots \\
\mathrm{BMP}_{i,1} & \mathrm{BMP}_{i,2} & \dots & \mathrm{BMP}_{i,\ell} \\
\dots & \dots & \dots & \dots \\
\mathrm{BMP}_{n,1} & \mathrm{BMP}_{n,2} & \dots & \mathrm{BMP}_{n,\ell} \\
\hline
\end{array}
$$

  contains (Y, Y) if a **random** $x_{i,k} = 1$,
  and (N, N) if $x_{i,k} = 0$,
- each $\mathrm{BMP}_{j,k}$ in the jth row $j \neq i$ contains
  (Y, N) if $x_{j,k} = 1$,
  and (N, Y) otherwise.

The attack on *random* exponents

Let (g, y_M) is Mallet's ElGamal public key ($y_M = g^{x_M}$).

The attack on *random* exponents

Let (g, y_M) is Mallet's ElGamal public key ($y_M = g^{x_M}$).

- During the voting procedure in each $\mathrm{BMP}_{j,k}$ one of the exponents $\omega_{j,k,L}, \omega_{j,k,R}$ will be revealed according to voter's choice $c_{j,k} \in \{0, 1\}$.

The attack on *random* exponents

Let (g, y_M) is Mallet's ElGamal public key ($y_M = g^{x_M}$).

- During the voting procedure in each $\mathrm{BMP}_{j,k}$ one of the exponents $\omega_{j,k,L}, \omega_{j,k,R}$ will be revealed according to voter's choice $c_{j,k} \in \{0, 1\}$.
- Let

$$K^*_\alpha = h_\alpha(y_M^{\omega_{n,\ell,L}}, y_M^{\omega_{n,\ell,R}})$$

for hash functions h_α, $\alpha = L, R$.

The attack on *random* exponents

Let (g, y_M) is Mallet's ElGamal public key ($y_M = g^{x_M}$).

- During the voting procedure in each $\mathrm{BMP}_{j,k}$ one of the exponents $\omega_{j,k,L}, \omega_{j,k,R}$ will be revealed according to voter's choice $c_{j,k} \in \{0,1\}$.
- Let
$$K_\alpha^* = h_\alpha(y_M^{\omega_{n,\ell,L}}, y_M^{\omega_{n,\ell,R}})$$
for hash functions h_α, $\alpha = L, R$.
- we shall see that
only the VM and Mallet can calculate keys K_α^*

The attack on *random* exponents

Recovering key:

$$K_{\alpha}^{*} = h_{\alpha}(y_M^{\omega_{n,\ell,L}}, y_M^{\omega_{n,\ell,R}})$$

The attack on *random* exponents

Recovering key:

$$K_\alpha^* = h_\alpha(y_M^{\omega_{n,\ell,L}}, y_M^{\omega_{n,\ell,R}})$$

- The VM knows Mallet public key y_M and the exponents used,

The attack on *random* exponents

Recovering key:

$$K^*_\alpha = h_\alpha(y_M^{\omega_{n,\ell,L}}, y_M^{\omega_{n,\ell,R}})$$

- The VM knows Mallet public key y_M and the exponents used,
- Mallet can rise first components $g^{\omega_{n,\ell,L}}$, $g^{\omega_{n,\ell,R}}$ of the ciphertexts in the pair $BMP_{n,\ell}$ to power x_M, and get $y^{\omega_{n,\ell,L}}$, $y^{\omega_{n,\ell,R}}$

The attack on *random* exponents

Recovering key:

$$K^*_\alpha = h_\alpha(y_M^{\omega_{n,\ell,L}}, y_M^{\omega_{n,\ell,R}})$$

- The VM knows Mallet public key y_M and the exponents used,
- Mallet can rise first components $g^{\omega_{n,\ell,L}}$, $g^{\omega_{n,\ell,R}}$ of the ciphertexts in the pair $BMP_{n,\ell}$ to power x_M, and get $y^{\omega_{n,\ell,L}}$, $y^{\omega_{n,\ell,R}}$
- only one (not both) of the $\omega_{n,\ell,L}$, $\omega_{n,\ell,R}$ will be revealed.

The attack on *random* exponents - encoding messages

Consequently, each other pair of exponents $\omega_{j,k,L}, \omega_{j,k,L}$ might carry a ciphertext:

$$\omega_{j,k,\alpha} = E_{K^*_\alpha}(m^*_{j,k}),$$

where E is a symmetric encryption scheme, and $m^*_{j,k}$ a message to be hidden in the $\mathrm{BMP}_{j,k}$.
So, a single ballot may carry $n \cdot \ell - 1$ messages to Mallet.

Other attacks on Neff's scheme

Other our attacks exploit:

- (supposed to be) random bits $x_{j,k}$, which decide on (Y, N),
- if a random BSN (*Ballot Sequence Number*) is assigned to each ballot (as stated in *VoteHere*), then also the BSNs may carry a kleptographic message,
- the order of precomputed $g^{\omega_{j,k,\alpha}}$ might point out one of $2n\ell$ messages, which might be kleptographically hidden by a permutation

$$\pi = H\left(\prod_{j=1}^{n} \prod_{k=1}^{\ell} \prod_{\alpha \in \{L,R\}} y^{\omega_{j,k,\alpha}}\right),$$

where H is a cryptographically strong hash function.

Outline

The countermeasure: make things verifiable

- avoid unnecessary randomness
  (e.g. a ballot output batch always put in lexicographic order).
- Produce random values from signatures (in Chaum's manner):

$$r = \mathcal{R}(\mathrm{sig}(h(q))),$$

  where:
  - $\mathcal{R}$ is a strong pseudorandom number generator,
  - sig is a <u>deterministic</u> signature scheme,
  - h is a cryptographically strong hash function,
  - q is a number present on the ballot (e.g. $q = \mathrm{BSN}$).
- Make future parameters (like BSN)
  dependent on current choices – use linear linking.

The countermeasure: two devices principle

- kleptography may break down (as far as we know now), if two independent devices are applied
  say one from USA (CIA) and one from Germany (BND)
- re-designing the protocols?

Conclusion

A critical requirement for e-voting systems:

... the offer must contain an evidence that the system proposed is immune against kleptographic attacks...